Las pasarelas de la industria de la vigilancia y su relación con los gobiernos mexicanos: escenarios 2015

Sumario.
1. Contexto 2. Los eventos comerciales de la industria de la vigilancia durante 2015 3. Desafíos para la ciudadanía y exigencias a los gobierno 4. Acciones emprendidas

1. Contexto

Recientes reformas legales[1] ampliaron las facultades de vigilancia del Estado mexicano que se suman a las capacidades de vigilancia que agencias de Estados Unidos tienen sobre las comunicaciones realizadas en México,[2] sin embargo, la constitucionalidad de dichos cambios legislativos está aún por ser revisada por la Suprema Corte de Justicia de la Nación. En este contexto afirmamos la vigencia del derecho a la inviolabilidad de las comunicaciones privadas establecido en el artículo 16 constitucional que, de acuerdo con interpretaciones recientes de la Suprema Corte, extiende su protección a los metadatos.

Con inversiones millonarias de presupuesto público, los gobiernos en México figuran entre los principales consumidores mundiales de tecnología para la vigilancia de las comunicaciones.[3] Las potenciales capacidades de intrusión de estas tecnologías han sido debatidas internacionalmente por los efectos negativos que generan en términos de privacidad y de vulneración a los derechos humanos.[4]

Este aumento en las capacidades de vigilancia no ha demostrado tener efecto en mejorar la seguridad de las personas,[5] ni haber tenido impacto en la eficiencia de las instituciones para garantizar la reducción del crimen organizado. Al no contar con evidencia pública de su utilidad, resulta imposible evaluar la idoneidad y pertinencia de dichas políticas públicas. Sobre el gasto público[6] destinado a la vigilancia se construye un pernicioso círculo de opacidad no susceptible a la rendición de cuentas gubernamentales y por lo tanto la compra de equipos de espionaje por el gobierno parece ser un tema excluido del debate democrático. El círculo de opacidad se cierra, con las excepciones de acceso a la información creadas bajo el argumento de seguridad nacional, que retrasa por años el

---

1 Al Código Nacional de Procedimientos Penales 2013 y a la Ley Federal de Telecomunicaciones 2014.

2 Sobre los programas del Departamento de Estado y de la DEA para almacenar los registros de las llamadas de países vecinos: http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/

3 Mexico Was Hacking Team's No. 1 Client for Spyware, Global Voices: https://advox.globalvoices.org/2015/07/10/mexico-was-hacking-teams-no-1-client-for-spyware/

4 Report on Internet surveillance technologies in Mexico: https://contingentemx.files.wordpress.com/2014/11/against-mexico_english.pdf

5 http://www.wsj.com/articles/common-crime-in-mexico-remained-steady-in-2014-survey-shows-1443645580

6 Inversión del gobierno mexicano en software de Hacking Team (Tablas y cifras) https://cl.ly/bsDV

conocimiento público sobre las adquisiciones, la integración de los órganos responsables de la vigilancia, los protocolos, resultados y las evaluaciones de las políticas y su implementación.

2. Los eventos comerciales de la industria de la vigilancia durante 2015

Las ferias comerciales son un espacio en el que es posible observar las dinámicas, los actores y los discursos que se construyen en torno a la seguridad y en el que manifiestan los fundamentos de las políticas públicas. Las autoridades del Estado validan la industria y sus prácticas a través de la participación y promoción de estos eventos. A través de esta legitimación se articulan los intereses comerciales con las políticas de seguridad de los gobiernos y los presupuestos asignados para impulsar la adquisición e implementación de capacidades de vigilancia.

Mediante la asistencia a los eventos, el acopio de información publicada y el intercambio de correos con los organizadores, hemos documentado la realización de cuatro ferias comerciales e la industria de la vigilancia realizados o por realizarse en México durante 2015:

1. Expo Seguridad, 28 al 30 de abril, Centro Banamex, México, D.F.
http://www.exposeguridadmexico.com/en/2.

2. Mexico Corporate Security Forum, 14 al 16 de octubre, Hotel Sheraton, México, D.F.
http://www.mexicosecurityforum.com/

3. ISS World Latin America, 20 al 22 de octubre, Hotel Hyatt, México, D.F.
http://www.issworldtraining.com/ISS_LA/index.htm

4. Mexico Security Summit 2015 (MexSec), 3 al 5 de noviembre, México D.F
http://enjambre.net/sites/default/files/mex-sec.pdf

a. Expo Seguridad. 28 al 30 de abril

Esta feria se realizó del 26 al 28 de abril de 2015 y fue inaugurada por Miguel Ángel Mancera, Jefe de Gobierno del Distrito Federal. Este evento se anunció como "el mejor emplazamiento para descubrir nuevos productos y conocer las tendencias más avanzadas en seguridad". El sitio web de la feria orgullosamente exhibía los apoyos de la Secretaría de Seguridad Pública del DF, la Procuraduría General de Jusicia del DF, la Comisión Nacional de Seguridad entre otras agencias. En la Expo Seguridad colocaron stands empresas como Hacking Team y Obses de México, S.A. de C.V. quienes comercializaron el pasado el software FinFisher. Exposeguridad promovió una línea de nuevos productos disponibles para las agencias del gobierno y corporaciones.

b**. Mexico Corporate Security Forum. 14 al 16 de octubre**

Esta reunión comercial de la industria de la vigilancia se promocionó como una oferta para “compañías que buscan de beneficiarse de las grandes oportunidades de inversión deben asegurar que su seguridad corporativa puede ser evaluada, planeada y ejecutada de forma holística y que cuente con la participación de los servicios de Seguridad Nacional para garantizar la seguridad de sus operaciones en México”, para combatir la “violencia relacionada con los carteles de la droga continúan llamando la atención de las compañías internacionales y de sus potenciales inversores. Homicidio, extorsión y el ataque a instalaciones tienen el potencial de impactar los procesos de la cadena de valor”.

Dentro de sus oradores principales anunciaron al Comisionado Nacional de Seguridad, al Director General de Seguridad Privada de la Comisión Nacional de Seguridad y al Jefe de Seguridad de la Información de la petrolera estatal mexicana PEMEX.

Entre sus patrocinadores estuvieron Ceberus, IPS, Raytheon Websense, Centro de Seguridad Industrial y la AMIPCI.

c. Intelligence Support Systemes Cyberintelligence Gathering (ISS) 20 al 22 de octubre

ISS World es la feria más grande a nivel global orientada a la oferta de servicios de alta tecnología para apoyar las tareas de inteligencia, análisis y vigilancia electrónica. En su versión para América Latina, el ISS World Latin America, también constituye la mayor reunión de la industria. Entre sus clientes se encuentran tanto las distintas entidades gubernamentales como los operadores de telecomunicaciones responsables de la intercepción y recopilación de información de las redes de telecomunicaciones. El costo de asistencia a evento era de 1,295 dólares por persona, con opción de llevar un invitado gratis.

En esta reunión se ofrecen seminarios de capacitación en torno a los temas, productos y servicios. Entre los tópicos que se discuten en las sesiones agendadas se encuentran la investigación en redes sociales e internet, la geolocalización de dispositivos, el reconocimiento facial, datos biométricos de voz, intrusiones pasivas, activas y remotas, recolección, almacenamiento y análisis de llamadas, monitoreo en tiempo real, acceso a contenido cifrado, navegación en la red profunda. En su descripción mencionan lia capacidad de enfrentar ataques de criminales, “hacktivistas” o intervenciones de redes WiFi. [7]

El principal patrocinador de este evento es la empresa Trovicor, junto a otras empresas como Hacking Team y FinFisher, de Gamma International[8] . Estas compañías se encuentran en la lista de las empresas

7 http://www.issworldtraining.com/ISS_LA/Brochure.pdf

8 FinFisher, el producto estrella de Gamma International, filial de Gamma Group encargada de ofrecer equipo y software de vigilancia. FinFisher es una

enemigas de internet elaborada por la organización Reporteros Sin Fronteras (RSF)[9][10][11]

d. Mexican Security Summit (MexSec 2015). 3 al 5 de noviembre

Organizada por la empresa Defence IQ asistir tiene un costo de 3,649 dólares. La reunión llamada MexSec 2015 representa el punto más elevado de la colaboración de la industria de la vigilancia con los gobiernos. Participarán en ella oficiales de Home Land Security de EU, Militares de los Gobiernos de México, El Salvador, Guatemala y Colombia y contará con participación de agencias de la ONU. Según su propaganda, la conferencia "busca apoyar las políticas y estrategias alineadas en los Planes de Defensa desarrollados por las agencias gubernamentales en México. De igual forma, busca consolidarse como una plataforma que permita el buen y eficiente intercambio de información entre las organizaciones de seguridad, la integración y cooperación entre las agencias mexicanas"

El brochure de MEXSEC que es enviado por correo electrónico una vez te registras para solicitar una invitación contiene una carta del Exsecretario de Marina Almirante Mariano Saynes quien sostiene:

> *"MEXSEC provee un foro ideal y una oportunidad para conocer a los líderes militares de México y otras partes del mundo. Venga con nosotros para lo que promete ser una experiencia estimulante".*

La lista de participantes confirmados son:

- Mayor General Manuel Augusto López Ambrosio
  Ministro de Defensa Nacional, Presidente del Consejo Superior CFAC, Guatemala
- Major General David Victoriano Munguia Payes
  Ministro de Defensa Nacional, República de El Salvador
- Enrique Francisco Galindo Ceballos
  Comisionado General de Policía Federal, CNS
- H.E. Ambassador Adam Blackwell
  Secretary of Multidimensional Security, OAS
- C. General de Brigada Juan Manuel Rico Gámez

suite de software espía muy sofisticada que se vende exclusivamente a los gobiernos con fines de inteligencia y de aplicación de la ley. Aunque se comercializa como una herramienta para la lucha contra la delincuencia, el spyware ha sido identificado como instrumento para una serie abusos de vigilancia por parte de diversos gobiernos a nivel mundial. (Citizen Lab, 2015) En su último reporte, el centro de investigación de la Universidad de Toronto, el Citizen Lab, denunció por segunda ocasión, la existencia de este software en nuestro país. https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

9 Hacking Team es conocida principalmente por Galileo http://www.hackingteam.it/images/stories/galileo.pdf , un software que control remoto imperceptible para el usuario, que permite romper el cifrado, tomar el control de los dipositivos independientemente de su sistema operativo, evadir cualquier tipo de software antivirus o cortafuegos instalados, recoger datos y mantener el seguimien
to de las personas sin importar su localización.http://contingentemx.net/2014/03/03/spyware-de-la-empresa-hacking-team-opera-bajo-redes-mexicanas/ La capacidad del software permite, por ejemplo, activar remotamente micrófonos y cámaras, identificar la ubicación y las relaciones de los "objetivos" de vigilancia. http://surveillance.rsf.org/en/hacking-team/ La compra de este software ha sido evidenciada a través de documentos recientes y ha sido denunciada por Citizen Lab (2014) https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

10 https://surveillance.rsf.org/en/trovicor/

11 https://surveillance.rsf.org/en/hacking-team/

Subjefe de Inteligencia Militar, SEDENA

- General Rodolfo Palomino López
  Director General, Policía de Colombia
- C. Vicealmirante CG. DEM. Juan Espinosa Orozco
  Director del Área de Inteligencia, SEMAR
- Mr. R. Gil Kerlikowske
  Commissioner U.S. Customs and Border Protection, USA
- Sr. Rubén Moreira Valdez
  Gobernador, Estado de Coahuila de Zaragoza
- Antonio L. Mazzitelli
  Director oficina México, UNODC

3. Desafíos para la ciudadanía y exigencias a los gobiernos

- Las capacidades crecientes de vigilancia de los gobiernos deben someterse al control democrático ejercido mediante diferentes procedimientos legales y herramientas ciudadanas que deben ser eficaces en un marco amplio de rendición de cuentas.

- Se cierne sobre México una tendencia negativa en materia de transparencia y rendición de cuentas relacionada con las capacidades de vigilancia de los gobiernos alimentada por las teorías de la seguridad nacional y un recrudecimiento de las leyes de carácter represivo. La sociedad civil en México debe actuar e involucrarse en exigir mayor rendición de cuentas de gobiernos en camino de consolidación de un estado mayor de vigilancia que por definición es incompatible con la democracia.

- En este contexto la industria mundial de la vigilancia ha visto en México terreno fértil para negocios multimillonarios, sin reparar en las consecuencias y el impacto del uso de las tecnologías en la vida de millones de personas en un marco de creciente corrupción y violencia.

- Un desafío fundamental es la complicidad de las autoridades del Estado y la industria de la vigilancia que se observa en los eventos comerciales ocurridos durante 2015. Los intereses comerciales se articulan con las políticas de seguridad de los gobiernos y año con año millones y millones del presupuesto público fluyen hacia empresas que ofrecen soluciones tecnológicas para reducir el crimen, cuando el crimen en realidad aumenta en México.

Enjambre Digital

ContingenteMX

4. Acciones emprendidas

A partir de esta coyuntura consideramos necesario emprender acciones para exigir la transparencia sobre la participación y el presupuesto invertido en compras y actividades relacionadas con los productos y servicios adquiridos en estas ferias comerciales por parte de las dependencias de los gobiernos mexicanos. A fin de contribuir con datos que nos permitan abrir un debate informado sobre este tema, hemos realizado treinta solicitudes de información pública en torno a los siguientes puntos:[12]

> *1. Los servidores públicos asistentes a los eventos comerciales de tecnología de la vigilancia realizados en México durante 2015.*
> *2. El monto de los recursos públicos erogados por concepto de inscripción, asistencia de servidores públicos y patrocinio a los eventos comerciales de tecnología de la vigilancia en 2015.*
> *3. La adquisición durante el presente ejercicio fiscal 2015, productos, servicios y/ o marcas de proveedores y/o fabricantes que se exhibieron en estas ferias durante 2015.*

Esperamos que este ejercicio aporte elementos para el diálogo entre los distintos actores sociales e invite a la ciudadanía a participar activamente en esta discusión.

Ciudad de México, 22 de cctubre 2015.

Enjambre Digital
www.enjambre.net
digital@enjambre.net

ContingenteMx
www.contingtentemx.net
contingentemx@autistici.org

12 0410 0000 36915 0410 0000 37015 0410 0000 37115 0210 0001 51315 0210 0001 51415 0210 0001 51515 0411 1000 87115 0411 1000 87215 0411 1000 87315 0001 3000 78515 0001 3000 78615 0001 3000 78715 1857 2002 63315 1857 2002 63515 1857 2002 63615 0001 7003 64315 0001 7003 64415 0001 7003 64615 0413 1001 43115 0413 1001 43215 0413 1001 43315 0000 9002 98515 0000 9002 98615 0000 9002 98715 2210 3000 58415 2210 3000 58515 2210 3000 58615 0000 7001 88615 0000 7001 88715 0000 7001 88815

Referencias

Citizen Lab (October 15, 2015). Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation.
https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

Citizen Lab (2014). Mapping Hacking Team's "Untraceable" Spyware.University of Toronto.
https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/

Godoy, E. (octubre, 2015). México, sede de expo sobre armas digitales.
Proceso. http://www.proceso.com.mx/?p=417126

Internews (2014) Informe sobre las tecnologías de la vigilancia de Internet en México.
https://contingentemx.files.wordpress.com/2014/11/boletin-inter.pdf

Reuters (Octubre 12, 2015). Mexico ramps up surveillance to fight crime, but controls lax.

http://ca.reuters.com/article/topNews/idCAKCN0S61WY20151012

Wikileaks Repository on Hacking Team
https://wikileaks.org/hackingteam/emails/